

Express Mail No.: 35615665US
International Application No.: PCT/SG02/000245
International Filing Date: October 21, 2002
Preliminary Amendment Accompanying
Substitute Specification

Rec'd PCT/PTO 18 APR 2005
10/531843

Amendments to the Abstract:

Please replace the previous Abstract with the following redlined Abstract:

ABSTRACT OF THE DISCLOSURE

~~Apparatus is disclosed which is~~ An apparatus arranged to accept digital data as an input, and to process ~~said the~~ data according to one of either the Secure Hash Algorithm (SHA-1) or Message Digest (MD5) algorithm to produce a fixed length output word. The apparatus includes a plurality of rotational registers for storing data, one of the registers ~~being~~ arranged to receive the input data, and data stores for ~~initialisation~~ initialization of some of ~~said the~~ plurality of registers according to whether the SHA-1 or MD5 algorithm is used. The data stores include fixed data relating to SHA-1 and MD5 operation. Also included is a plurality of dedicated combinatorial logic circuits arranged to perform logic operations on data stored in selected ones of ~~said the~~ plurality of registers.